WLCとNACゲストサーバ(NGS)の統合ガイド

内容

概要

このドキュメントでは、NAC ゲスト サーバとワイヤレス LAN コントローラの統合に関するガイドラインを示します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ワイヤレス LAN コントローラ（WLC）4.2.61.0
- IOS® バージョン 12.2(25)SEE2 を実行する Catalyst 3560
- Cisco ADU バージョン 4.0.0.279
- NAC ゲスト サーバ バージョン 1.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

Cisco NAC ゲスト サーバは、ゲスト、訪問者、契約者、コンサルタント、顧客等に一時的なネットワーク アクセスを提供する完成されたプロビジョニングおよびレポート システムです。ゲスト サーバは Cisco NAC アプライアンスまたは Cisco ワイヤレス LAN コントローラに近接して動作し、ゲスト アクセス用のキャプティブ ポータルと実施ポイントになります。

Cisco NAC ゲスト サーバにより、任意の特権ユーザは簡単に仮ゲスト アカウントとスポンサー ゲスト アカウントを作成できます。Cisco NAC ゲスト サーバはスポンサー（ゲスト アカウントを作成するユーザ）の完全認証を行い、スポンサーは印刷物、電子メール、または SMS によりアカウントの詳細をゲストに通知できるようになります。ユーザ アカウントの作成からゲスト ネットワーク アクセスに至る一連の手続きはすべて監査およびレポート用に保存されます。

ゲスト アカウントが作成されると、Cisco NAC アプライアンス マネージャ（Clean Access Manager）内でプロビジョニングされるか、または Cisco NAC ゲスト サーバの組み込みデータベース内に保存されます。ゲスト サーバの組み込みのデータベースを使用すると、Cisco ワイヤレス LAN コントローラなどの外部ネットワーク アクセス デバイスでは、Remote Authentication Dial In User Service（RADIUS）プロトコルによってゲスト サーバに対してユーザを認証できます。

Cisco NAC ゲスト サーバでは、アカウント作成時に有効期間を指定してゲスト アカウントをプロビジョニングします。アカウントが失効すると、ゲスト サーバは、Cisco NAC アプライアンス マネージャからアカウントを直接削除するか、ネットワーク アクセス デバイス（NAD）でこのユーザを削除しなければならない時点までにこのアカウントに対して残されている有効期間を NAD に通知する RADIUS メッセージを送信します。

Cisco NAC ゲスト サーバでは、中央管理インターフェイスを通してレポートを実行できるように、ゲスト アカウントの作成からゲストによるアカウントの使用に至るすべての監査証跡を統合することより、ゲスト ネットワーク アクセス用アカウント管理機能を実現します。

ゲスト アクセスの概念

Cisco NAC ゲスト サーバでは、ゲスト アクセスを可能にするために必要なコンポーネントについて記述する目的で多数の用語を使用します。

ゲスト ユーザ

ゲスト ユーザは、ネットワークにアクセスするためにユーザ アカウントを必要とするユーザです。

スポンサー

スポンサーは、ゲスト ユーザ アカウントを作成する個人です。多くの場合、ネットワーク アクセスを提供する組織の従業員です。スポンサーは、特定の職務上の役割を持つ具体的な 3 人の個人にするか、Microsoft Active Directory（AD）などの企業のディレクトリに対して認証できる任意の従業員にすることができます。

ネットワーク エンフォースメント デバイス

これらのデバイスは、ネットワーク アクセスを提供するネットワーク インフラストラクチャ コンポーネントです。さらに、ネットワーク エンフォースメント デバイスは、ゲスト ユーザをキャプティブ ポータルにプッシュします。このポータルでゲスト ユーザはゲスト アカウントの詳

細を入力できます。ゲストが一時的なユーザ名とパスワードを入力すると、ネットワーク エンフォースメント デバイスでは、ゲスト サーバによって作成されたゲスト アカウントと照合して、このクレデンシャルをチェックします。

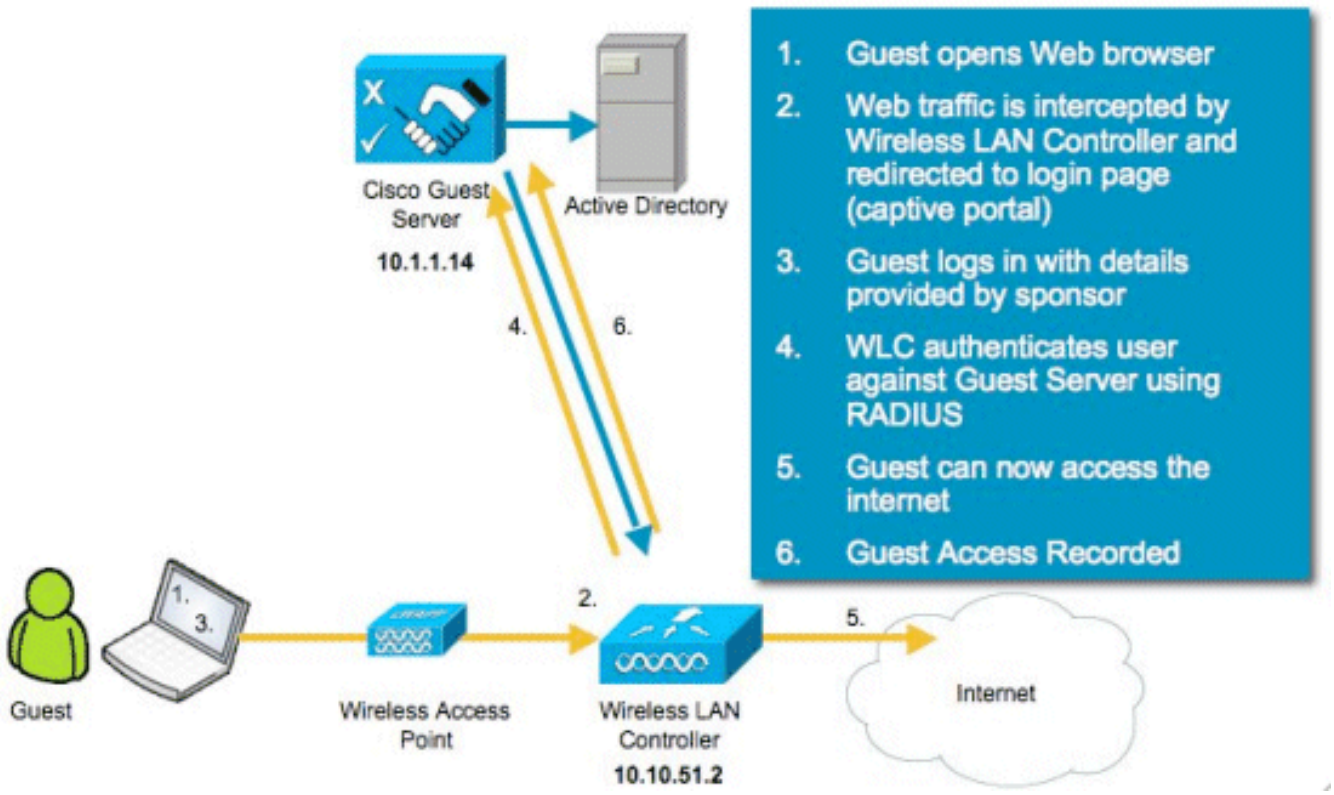
ゲスト サーバ

これは Cisco NAC ゲスト サーバです。ゲスト アクセスのすべての要素を 1 まとめにします。ゲストサーバは、ゲストアカウントを作成するスポンサー、ゲストに渡されるアカウントの詳細、ネットワークエンフォースメントデバイスに対するゲスト認証、ゲストサーバを使用したゲストのネットワークエンフォースメントデバイスの検証をリンクします。さらに、Cisco NAC ゲスト サーバは、ネットワーク エンフォースメント デバイスからのアカウント情報を統合することにより、ゲスト アクセス レポートの一元管理を実現します。

NGS の詳細な資料は CCO にあります。

http://www.cisco.com/en/US/docs/security/nac/guestserver/configuration_guide/10/nacguestserver.html

ラボ トポロジの概要



ワイヤレス LAN コントローラ (WLC) の設定

WLC を設定するには、次の手順を実行します。

1. コントローラとアクセス ポイントを初期化します。
2. コントローラ インターフェイスを設定します。
3. RADIUS を設定します。
4. WLAN 設定値を設定します。

初期化

初期設定の場合は、ハイパーターミナルなどのコンソール接続を使用し、セットアップ プロンプトに従ってログインおよびインターフェイス情報を入力します。**reset system コマンドによってもこれらのプロンプトが開始されます。**

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_44:36:c3]: WLC
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): admin
Service Interface IP Address Configuration [none][DHCP]: <ENTER>
Enable Link Aggregation (LAG) [yes][NO]:no
Management Interface IP Address: 10.10.51.2
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.51.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 2]: 1
Management Interface DHCP Server IP Address: 10.10.51.1
AP Transport Mode [layer2][LAYER3]: layer3
AP Manager Interface IP Address: 10.10.51.3
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (10.10.5<X>.1):<ENTER>
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: mobile-1
Enable Symmetric Mobility Tunneling: No
Network Name (SSID): wireless-1
Allow Static IP Addresses [YES][no]:<ENTER>
Configure a RADIUS Server now? [YES][no]:<ENTER>
Enter the RADIUS Server's Address: 10.1.1.12
Enter the RADIUS Server's Port [1812]:<ENTER>
Enter the RADIUS Server's Secret: cisco
Enter Country Code (enter 'help' for a list of countries) [US]:<ENTER>
Enable 802.11b Network [YES][no]:<ENTER>
Enable 802.11a Network [YES][no]:<ENTER>
Enable 802.11g Network [YES][no]:<ENTER>
Enable Auto-RF [YES][no]:<ENTER>
Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: yes
Enter the date in MM/DD/YY format: mm/dd/yy
Enter the time in HH:MM:SS format: hh:mm:ss
```

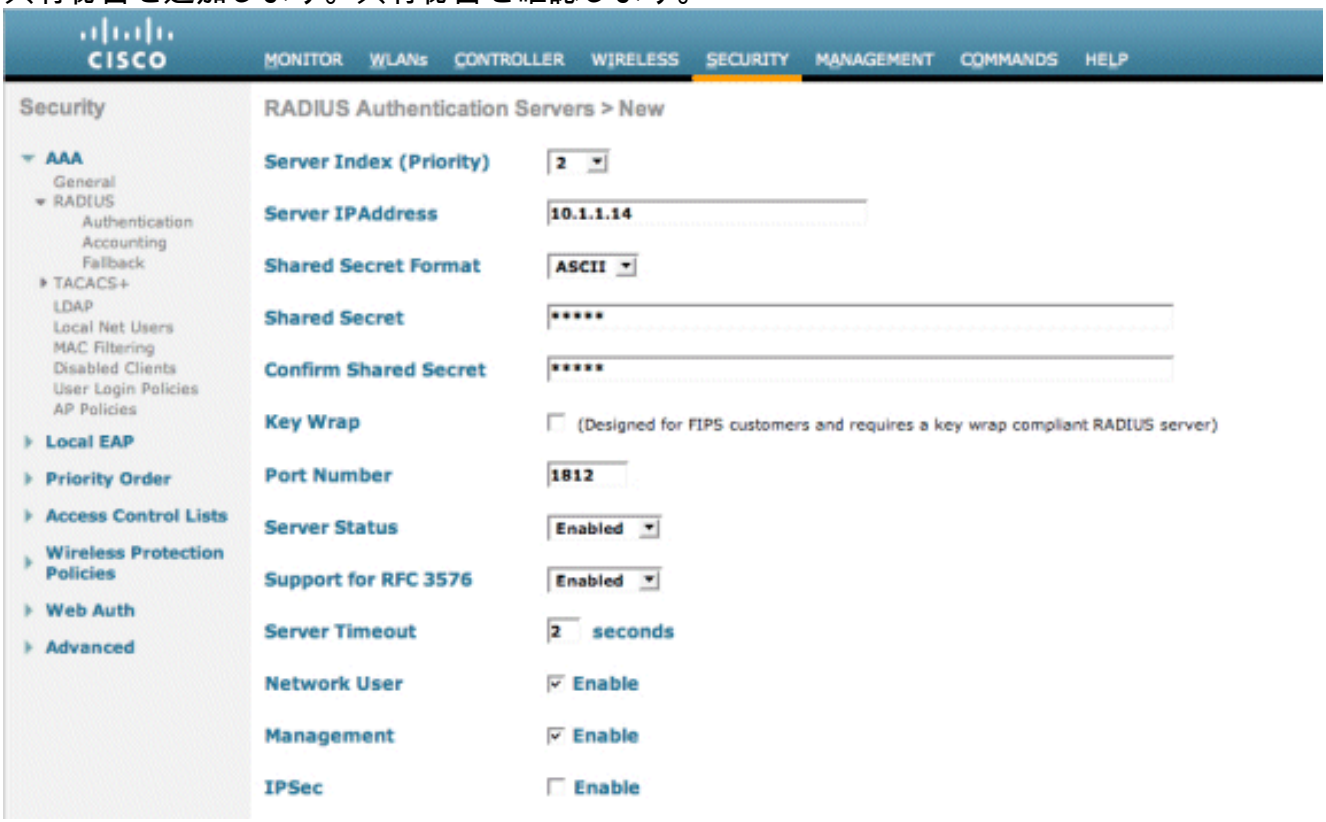
Cisco NAC Guest Server

Cisco NAC ゲスト サーバは、ゲスト、契約社員などのクライアントに一時的なネットワーク アクセスを提供するプロビジョニングおよびレポート ソリューションです。Cisco NAC ゲスト サーバは、Cisco Unified Wireless Network または Cisco NAC アプライアンス ソリューションとともに動作します。このドキュメントでは、 Cisco NAC ゲスト サーバを Cisco WLC と統合する手順を説明します。これにより、ゲスト ユーザ アカウントを作成し、ゲストの一時的なネットワーク アクセスを検証します。

統合を完了するには、次の手順を実行します。

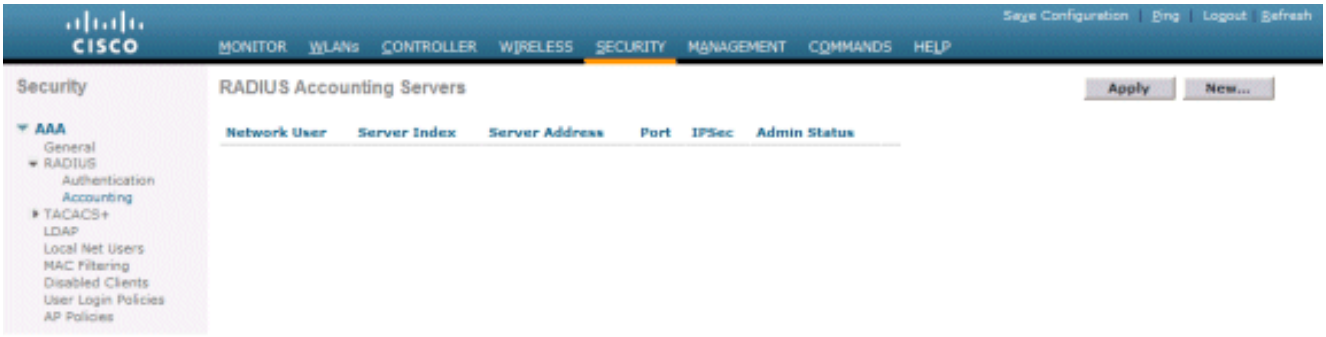
1. WLC で認証サーバとして Cisco NAC ゲスト サーバを追加します。これを設定するには、WLC（ https://10.10.51.2、admin/admin ）を参照します。[Security] > [RADIUS] > [Authentication] の順に選択します。

New を選択します。Cisco NAC ゲスト サーバの IP アドレス（10.1.1.14）を追加します。共有秘密を追加します。共有秘密を確認します。

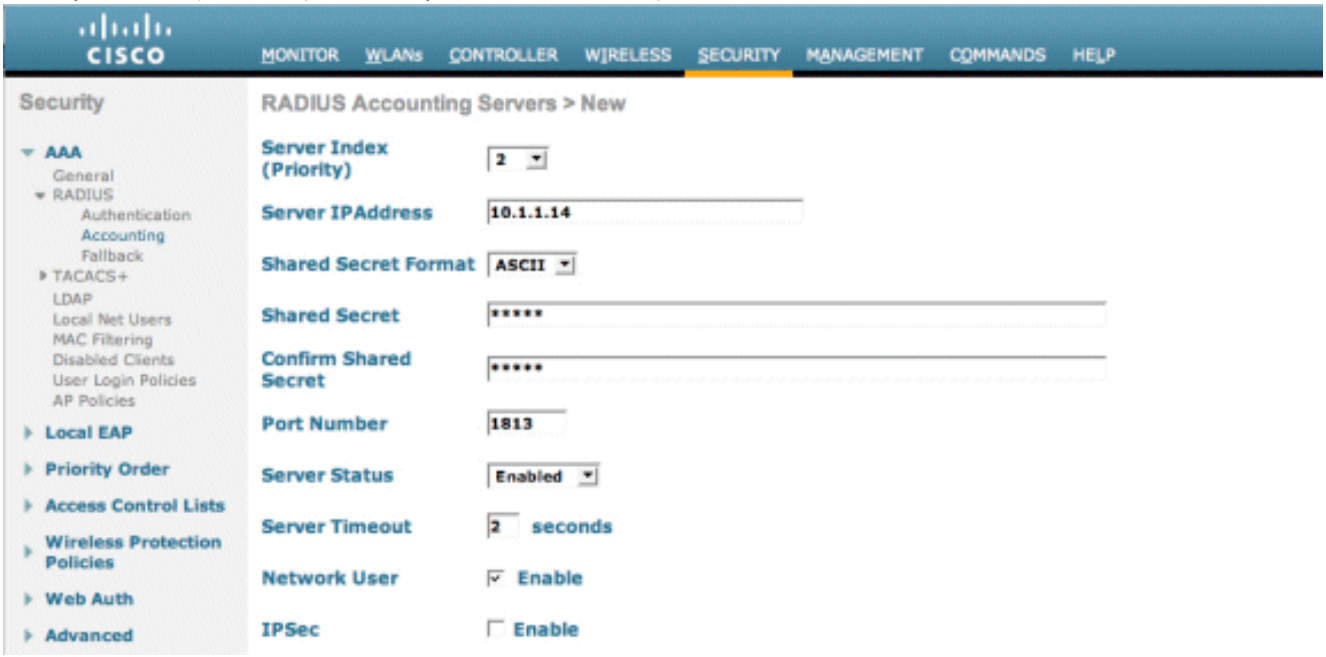


Apply を選択します。

2. WLC でアカウンティング サーバとして Cisco NAC ゲスト サーバを追加します。[Security] > [RADIUS] > [Accounting] を選択します。

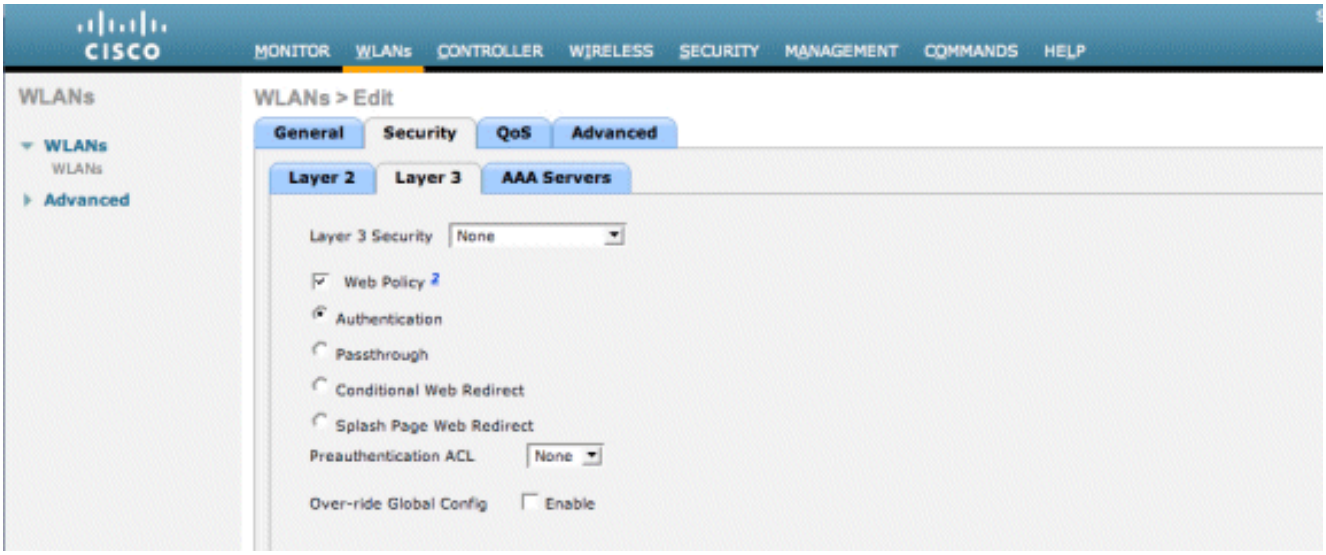


New を選択します。Cisco NAC ゲスト サーバの IP アドレス（10.1.1.14）を追加します。共有秘密を追加します。共有秘密を確認します。

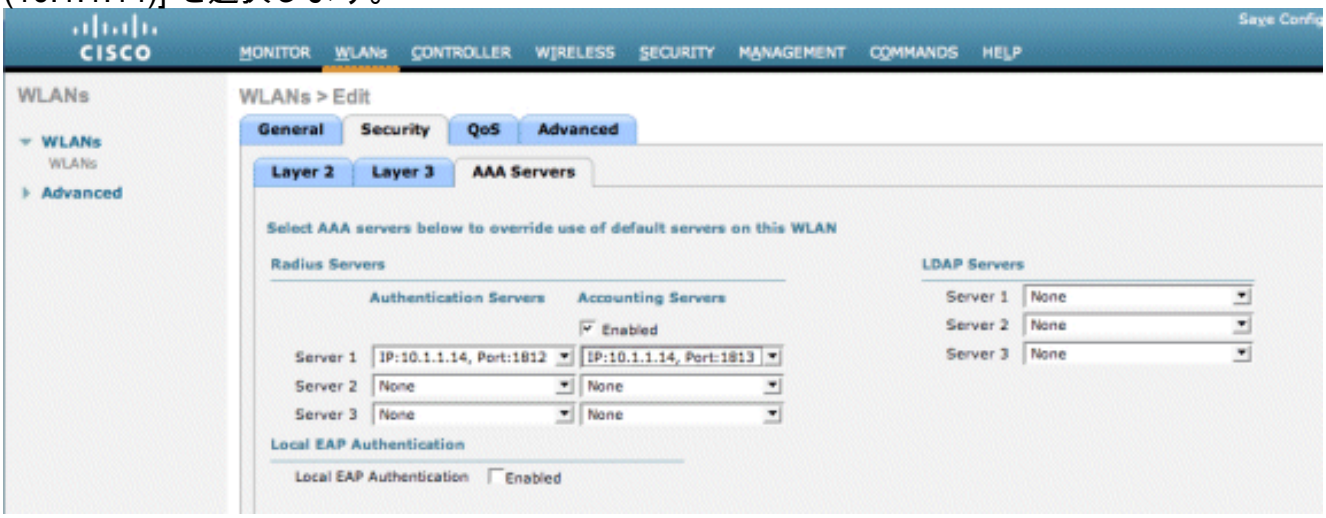


Apply を選択します。

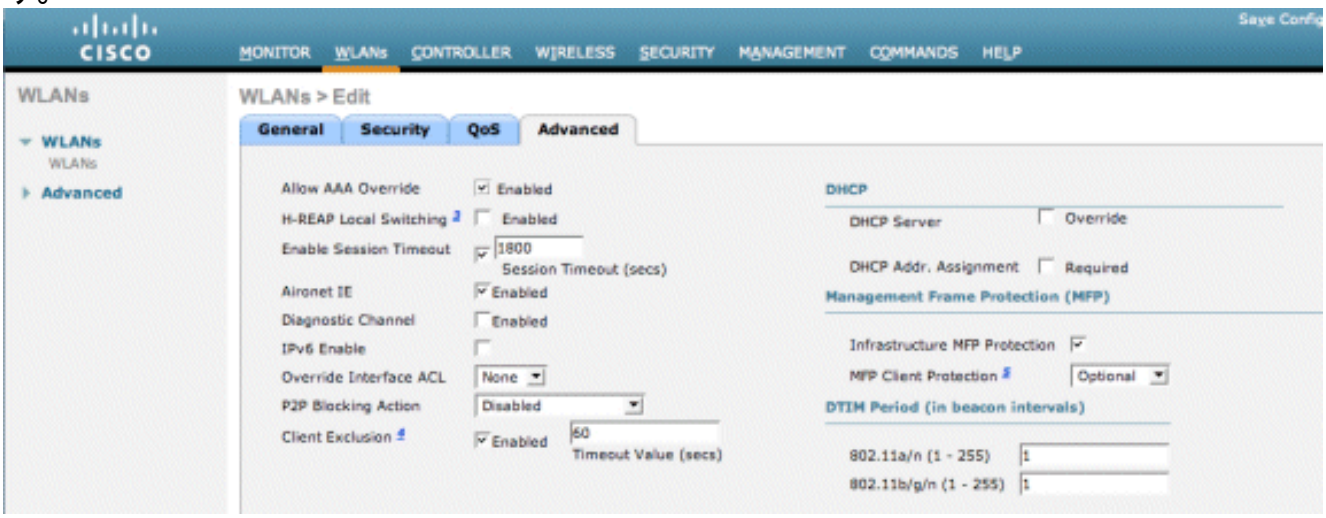
3. NAC ゲスト サーバを使用するように WLAN（wireless-x）を変更します。WLAN（wireless-x）を編集します。[Security] **タブを選択します。**[Layer 2 Security] を [None] に変更し、[Web Authentication] を使用するように [Layer 3 Security] を変更します。



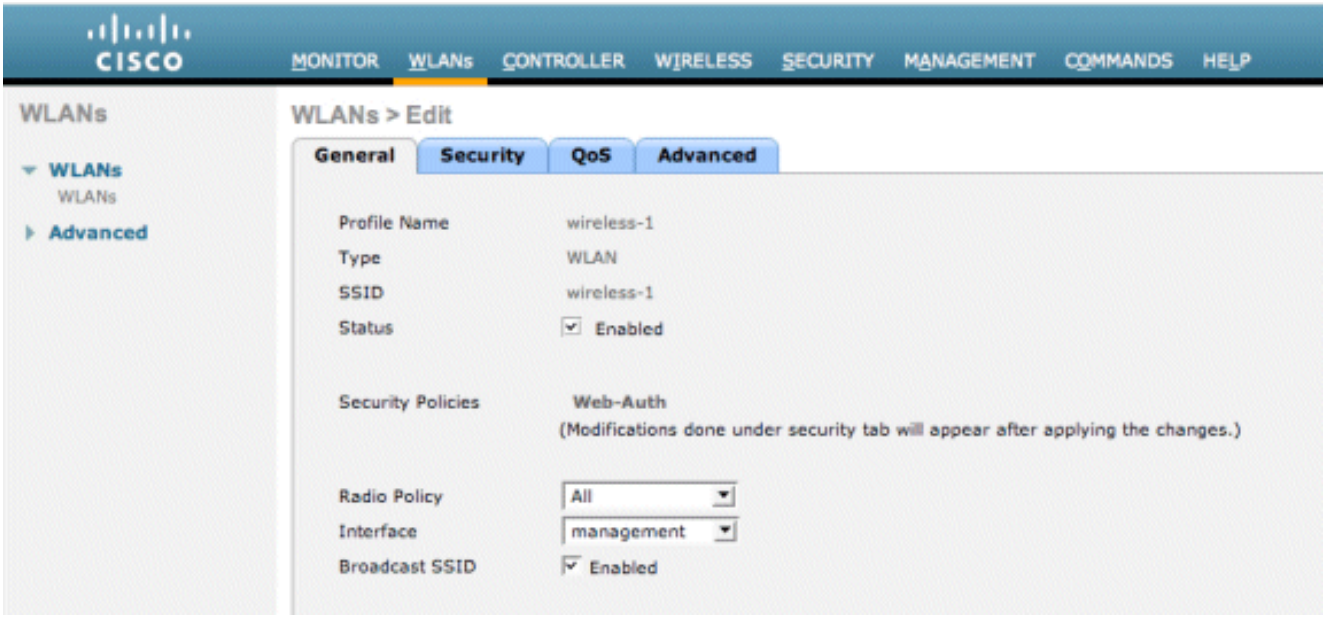
[Security] タブの下で [AAA Servers] **を選択します。**[Server 1] ボックスの下で、[RADIUS server (10.1.1.14)] を選択します。[Server 1] ボックスの下で、[Accounting Server (10.1.1.14)] を選択します。



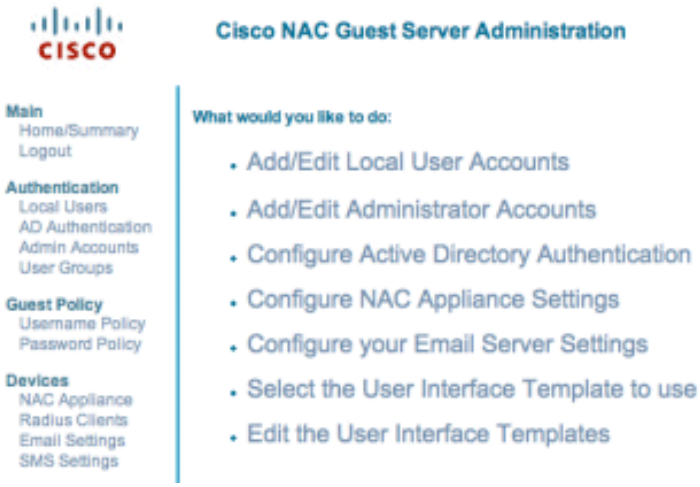
[Advanced] タブを選択します。[Allow AAA Override] をイネーブルにします。これにより、NAC ゲスト アプライアンスからクライアントごとのセッション タイムアウトを設定できます。



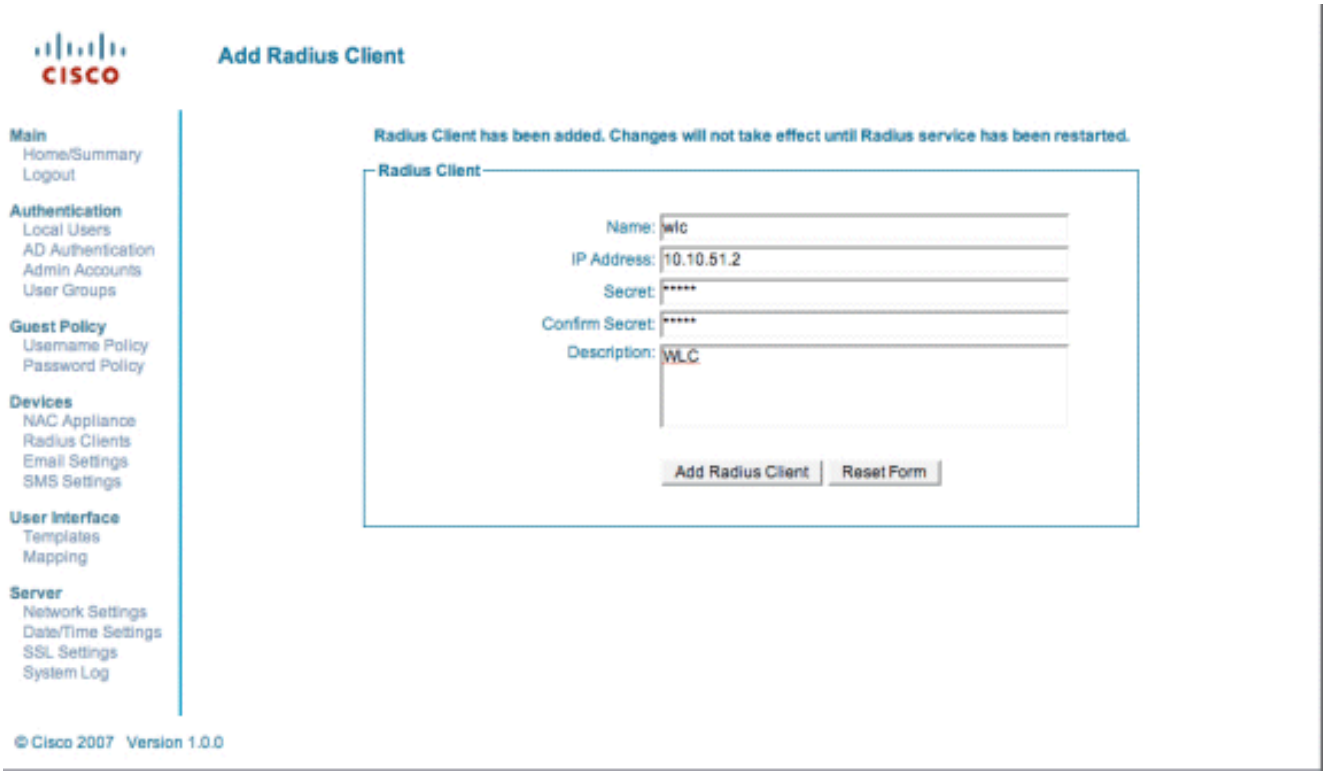
注：SSIDで**AAA override**が有効になっている場合、NGS上のゲストユーザの残りのライフタイムは、ゲストユーザのログイン時のセッションタイムアウトとしてWLCにプッシュされます。[Apply] を選択して WLAN 設定を保存します。



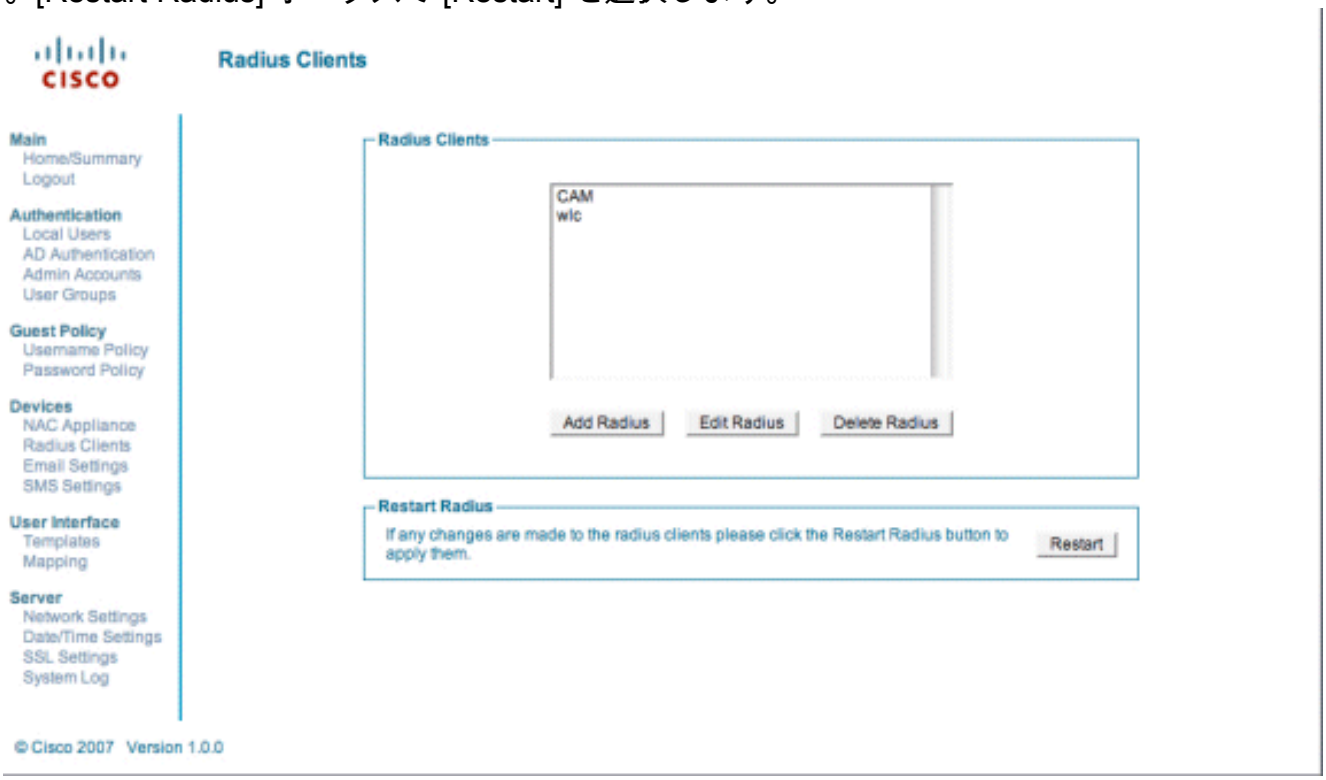
4. Cisco NAC ゲスト サーバに RADIUS クライアントとしてコントローラが追加されているかどうかを確認します。これを設定するには、NAC ゲスト サーバ（https://10.1.1.14/admin）を参照します。**注：URL**に/adminを指定すると、[Administration]ページが表示されます。



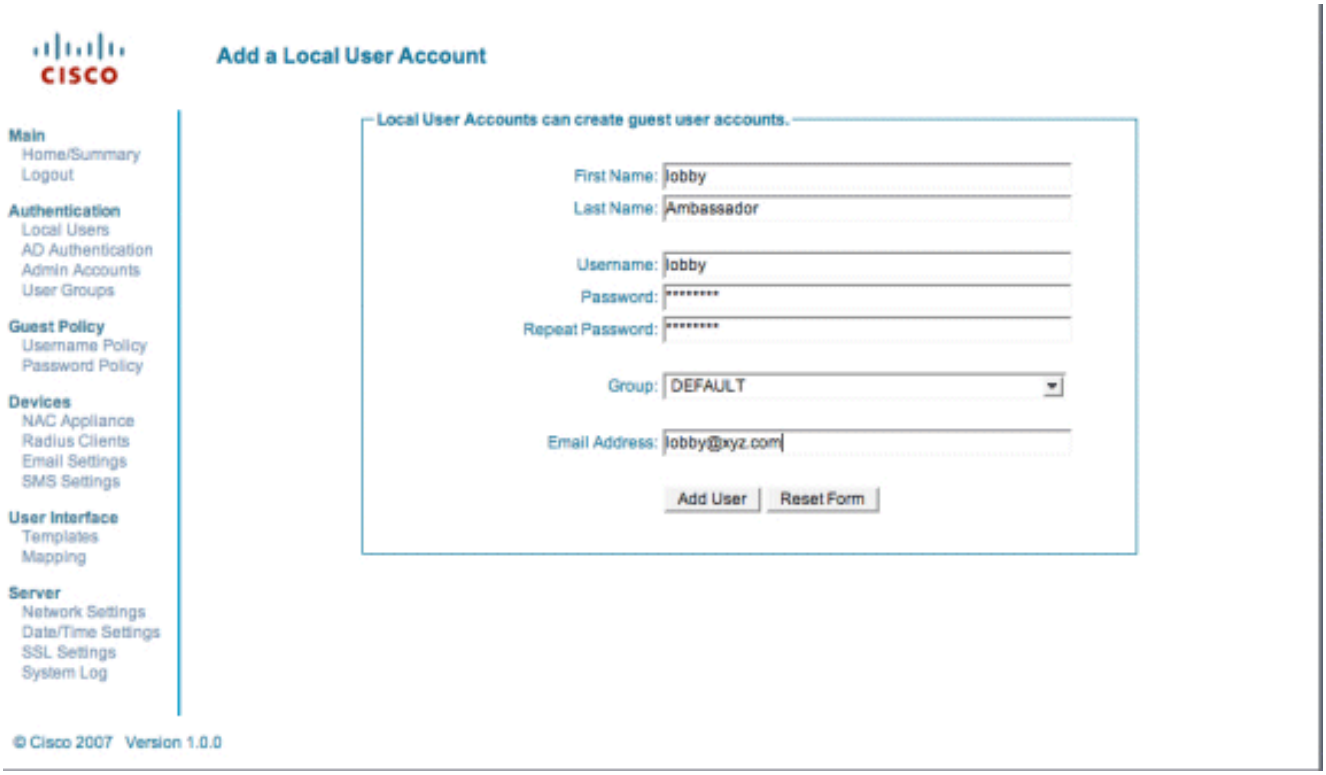
[Radius Clients] を選択します。[Add Radius] を選択します。RADIUS クライアント情報を入力します。名前（WLCシステム名）を入力します。IPアドレス(WLCのIPアドレス**(10.10.51.2)**)を入力します。ステップ 1 で入力した同じ共有秘密を入力します。共有秘密を確認します。説明を入力します。[Add Radius Client] を選択します。



変更を有効にするために RADIUS サービスを再起動します。[Radius Clients] を選択します。[Restart Radius] ボックスで [Restart] を選択します。

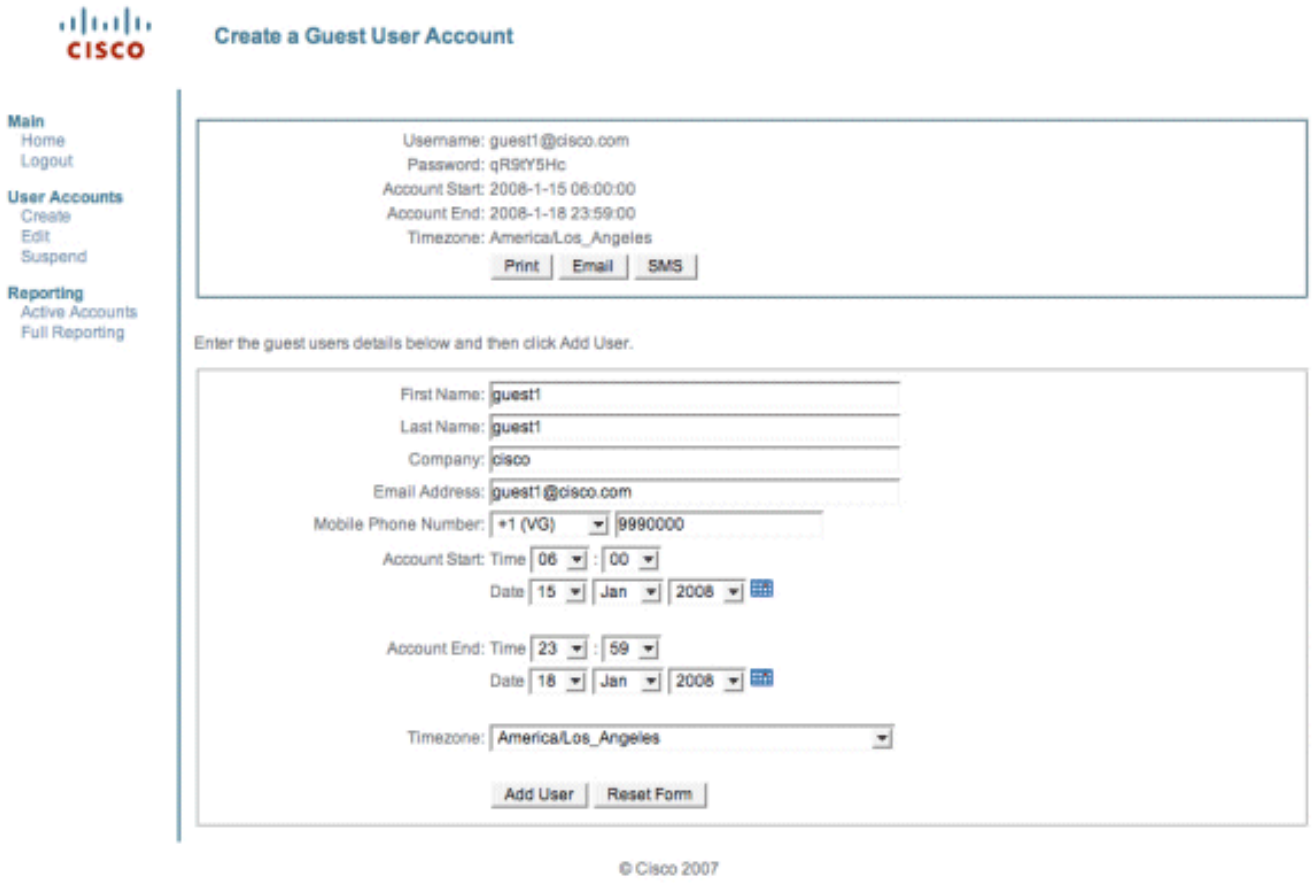


5. Cisco NAC ゲスト サーバにローカル ユーザ（Lobby Ambassador）を作成します。[Local Users] を選択します。[Add User] を選択します。**注：すべての**フィールドに入力する必要があります。[First Name]に**lobby**と入力します。[Last Name]に**Ambassador**と入力します。ユーザ名**lobby**を入力します。[Password]に**password**と入力します。[Group] を [Default] のままにします。電子メールアドレス**lobby@xyz.com**を入力します。[Add User] を選択します。



6. ローカル ユーザとしてログインし、ゲスト アカウントを作成します。NAC ゲスト サーバ（https://10.1.1.14）を参照し、ステップ 5 で作成したユーザ名とパスワードでログインして、これを設定します。

ゲスト ユーザ アカウントの [Create] を選択します。**注：すべての**フィールドに入力する必要があります。[First Name] を入力します。[Last Name] を入力します。[Company] を入力します。[Email Address] を入力します。**注：電子メール**アドレスはユーザ名です。[Account End: **Time**]を入力します。[Add User] を選択します。



7. ゲスト WLAN に接続し、ゲスト ユーザとしてログインします。ワイヤレス クライアントをゲスト WLAN (wireless-x) に接続します。Web ブラウザを開くと [Web-Auth Login] ページにリダイレクトされます。**注：または、https://1.1.1.1/login.html**と入力してログインページにリダイレクトすることもできます。ステップ 6 で作成したゲスト ユーザ名を入力します。ステップ 6 で自動生成されたパスワードを入力します。WLC に Telnet 接続し、**show client detail コマンドを使用して、セッション タイムアウトが設定されていることを確認します。**セッション タイムアウトが経過すると、ゲスト クライアントが接続解除し、ping が停止します。

```
(Cisco Controller) >show client detail 00:13:e8:b7:5e:dd
Client MAC Address.............................. 00:13:e8:b7:5e:dd
Client Username ................................ podx@cisco.com
AP MAC Address.................................. 00:17:df:a6:e5:f0
Client State.................................... Associated
Wireless LAN Id................................. 1
BSSID........................................... 00:17:df:a6:e5:ff
Channel......................................... 60
IP Address...................................... 10.1.1.22
Association Id.................................. 1
Authentication Algorithm........................ Open System
Reason Code..................................... 0
Status Code..................................... 0
Session Timeout................................. 59
Client CCX version.............................. 4
Client E2E version.............................. 1
Mirroring....................................... Disabled
QoS Level....................................... Silver
Diff Serv Code Point (DSCP)..................... disabled
802.1P Priority Tag............................. disabled
WMM Support..................................... Enabled
U-APSD Support.................................. Disabled
Mobility State.................................. Local
--More-- or (q)uit
(Cisco Controller) >
```

注：ワイヤレスLANコントローラ(WLC)からNACゲストサーバ(NGS)へのWeb認証を設定するには、Web認証プロパティでPAPモード認証を使用する必要があります。CHAP は NGS でサポートされていないため、Web 認証ポリシーが CHAP に設定されていると認証は失敗します。

関連情報

- 『Cisco NAC アプライアンス - Clean Access Manager インストレーションおよびコンフィギュレーション ガイド リリース 4.1(3)』
- 『Cisco NAC アプライアンス スイッチおよびワイヤレス LAN コントローラのサポート』
- Cisco Wireless LAN Controller コンフィギュレーション ガイド、リリース 7.0.116.0
- （ビデオ）Cisco Identity Services Engine（ISE）とワイヤレス LAN コントローラ（WLC）の統合
- NAC(Clean Access)：ゲストアクセスの設定
- 導入ガイド：Cisco Wireless LAN Controllerリリース4.1を使用したCiscoゲストアクセス
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。